

- в результаті перевірки транзакція або об'єднується з іншими аналогічними для створення нового блоку даних або відкидається;
 - новий блок додається до існуючого, таким чином, щоб він був постійним і незмінним;
 - транзакцію завершено.
- На рисунку 3 зображено послідовні етапи здійснення операцій у Blockchain на прикладі криптовалют.

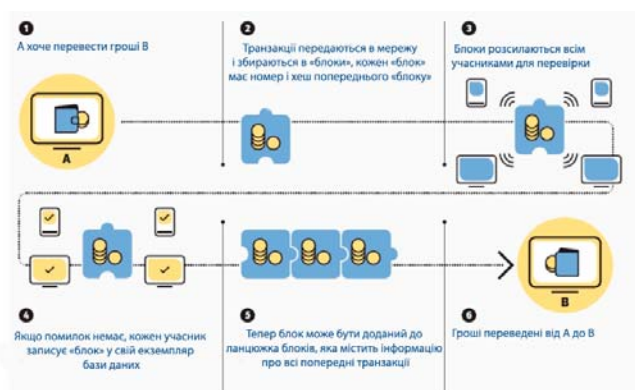


Рис. 3. Послідовність основних етапів проведення операцій (або транзакцій) технології Blockchain

Список використаних джерел

1. Інтернет речей [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Інтернет_речей.
2. Статистика інтернету речей [Електронний ресурс]. – Режим доступу: <https://www.statista.com>.
3. IoT и проблемы безопасности [Електронний ресурс]. – Режим доступу: <https://habr.com/ru/company/unet/blog/410849/>
4. What is Blockchain Technology? [Електронний ресурс]. – Режим доступу: <https://blockgeeks.com/guides/what-is-blockchain-technology/>

УДК 621.3

КЕРУВАННЯ СВІТЛОДІОДНОЮ RGB МАТРИЦЕЮ НА БАЗІ ПЛАТФОРМИ ARDUINO NANO V3.0 ЗА ДОПОМОГОЮ СМАРТФОНУ

Чеботар Б.Р., студент гр. КІ-1606

Шумська Л.М., керівник проекту, викладач-методист

*Чернігівський національний технологічний університет
Коледж транспорту та комп'ютерних технологій ЧНТУ*

Пристрої виводу інформації є одним із найпоширеніших типів представлення інформації і дозволяють отримувати інформацію у вигляді тексту, звуку, відео, фото і т. д.

Існує багато різноманітних пристроїв для візуального виводу інформації, наприклад: монітор, проектор, світлодіодні індикатори, матриці на світлодіодних індикаторах, рідкокристалічні дисплеї тощо.

Одним із цікавих напрямків виводу візуальної інформації є розробка пристроїв з використанням матриць на RGB світлодіодах.

RGB матриці можуть бути реалізовані з різними схемами керування: зі спільним анодом, зі спільним катодом, без спільного анода та катода, що допускає різні способи комутації (зазвичай випускається у вигляді SMD компонента). В RGB світлодіоді на одній підкладці встановлені незалежні кристали трьох кольорів світіння (R+G+B) [4].

Яскравість світлодіодів дуже добре піддається регулюванню, але не за рахунок зниження напруги живлення, що до речі не припустимо, а за допомогою методу широтно-імпульсної модуляції (ШІМ), для чого необхідний спеціальний керуючий блок (реально він може бути поєднаний з блоком живлення і конвертором, а також з контролером управління кольором RGB-матриці) [5].

Метод ШІМ полягає в тому, що на світлодіод подається не постійний, а імпульсно-модульований струм, причому частота сигналу повинна становити від сотень до тисяч герц, а ширина імпульсів і пауз між ними може змінюватися. Середня яскравість світлодіода стає керованою, в той же час світлодіод не гасне [5].

Конструктивне виконання матриць також є різноманітним, що дозволяє підібрати конкретну реалізацію для конкретного застосування в залежності від потреб. Це може бути виконання у вигляді квадратної матриці на жорсткій друкованій платі, на гнучкій підложці, різного формату. Було запропоновано використовувати RGB матрицю типу WS2812B.

Дуже зручно використовувати RGB матрицю з керуванням за допомогою смартфона. Для цього потрібно додатково використати мікроконтролер або платформу, наприклад, фірми Arduino, яка пропонує різноманітні платформенні набори з різноманітною периферією. Для даної реалізації було обрано Arduino

NANO v3.0, тому, що вона має невеликий розмір, функціонально завершена для базових завдань обробки вводу і виводу інформації, має достатню кількість роз'ємів підключення, в тому числі Mini-B USB. Живлення може здійснюватись через Mini-B USB

Дана платформа реалізована на базі мікроконтролера Atmega328P. Пам'ять мікроконтролера типу EEPROM має ємність 32 КБ і дозволяє завантаження нескладних програмних додатків. Для роботи з поточними даними є пам'ять SRAM ємністю 2 КБ.

Живлення здійснюється по виводам GND та 5V, напруга живлення може бути 3.3-12В. Підключення світлодіодної матриці здійснюється до виводу D6 з виходом на Din (рис. 1).

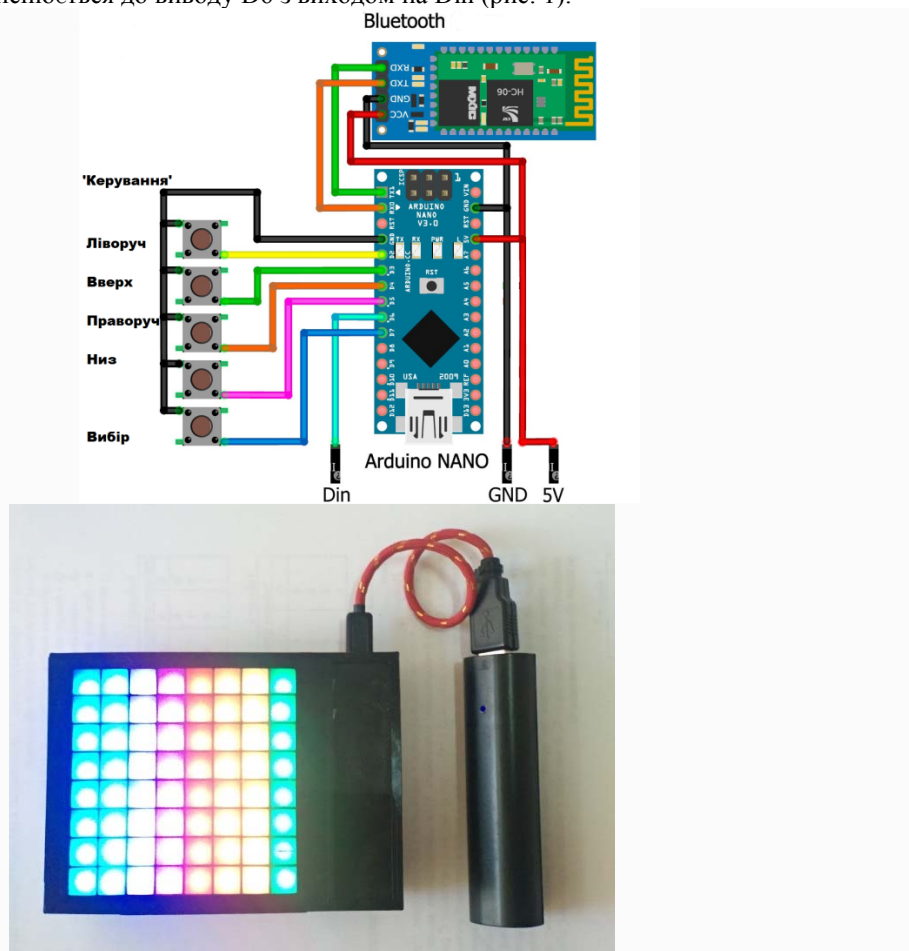


Рис.1. Підключення на матриці

Підключення на матриці здійснюється до виводу Din аналогічно з підключенням живлення по входах GND та 5V відповідно, підключення на матриці здійснюється послідовно з паралельним живленням.

Керування за допомогою смартфона здійснюється по Bluetooth каналу. Для цього потрібен Bluetooth модуль Wireless TTL Transceiver Module від MDFLY electronics [2].

Підключення модуля здійснюється до виводів RXD та TXD від виводів платформи Arduino NANO TX1 та RX0 відповідно. Модуль Bluetooth містить мікросхеми драйверів, що забезпечують роботу по Bluetooth інтерфейсу.

Для керування може використовуватися будь-який смартфон з будь-якою операційною системою. В даному проекті використовується смартфон Xiaomi miA1 з операційною системою Android 9.0. Налаштування полягає в завантаженні програми GyverMatrixBT, що надається у вільне користування [1].

При відкритті даної програми потрібно виконати опцію підключення Bluetooth, і програма готова до роботи.

Функціональні можливості є дуже широкими – можна вводити на смартфоні текст з подальшим виведенням на RGB матрицю, змінювати колір тексту, малювати з піксельним дозволом одного світлодіода, вставляти картинки, увімкнути анімацію, запустити нескладні ігри тощо. При роботі з ігровими додатками передбачено використання кнопок керування напрямом переміщення світлодіодних засвічувань.

Таким чином даний пристрій дозволяє різноманітно користуватися ним як в якості ігрового пристрою так і пристрою текстового та графічного виведення інформації з великою кількістю ефектів. Пристрій дозволяє регулювати періодичність повторень, частоту появи анімаційних ефектів та швидкість анімації завдяки програмному забезпеченню.

На базі даної платформи Arduino NANO можна розширити функціонал пристрою підключенням модулів виведення поточного часу, температури, інтенсивності освітлення і відповідно керуванням освітлювальними приладами, приладами обігріву, включення електроприладів за заданим часом або на заданий термін тощо.

Список використаних джерел

1. Google Play. Додатки [Електронний ресурс]. – Режим доступу: <https://play.google.com/store/apps/details?id=com.beragumbo.GyverMatrixBT>
2. MDFLY electronics New products. [Електронний ресурс]. – Режим доступу: <http://www.mdfly.com/>
3. Arduino контролери [Електронний ресурс]. – Режим доступу: <https://arduino.ua/prod166-arduino-nano-v3-0-avr-atmega328-p-20au-s-kabelem-mini-usb-i-raspyannimi-razyomami>
4. Трехцветные светодиоды RGB [Електронний ресурс]. – Режим доступу: <http://ledno.ru/svetodiody/trexcvetnye-rgb.html>
5. Усе про світло діоди [Електронний ресурс]. – Режим доступу: http://elektrotovary.te.ua/index.php?route=information/news&news_id=6
6. Светодиодная RGB матрица [Електронний ресурс]. – Режим доступу: <http://arduino.ua/prod340-svetodiодnaya-matrica-8h8-rgb-60mm>

УДК 004.056.55

THE PRINCIPLES OF MODERN MESSENGERS WORK FOR TRANSFER ENCRYPTED DATA

D. Shuliachenko, T. Chorny, students of group MCEs-171

Scientific supervisors: **S.V. Zaitsev**, Doctor of Technical Sciences, assistant professor
Chernihiv National University of Technology

There is a high competition in the area of messengers nowadays. The access to the Internet is not only on PC but also on smartphones. This fact allowed messengers to become the most popular app.

Each messenger has their audience which agitates to use exactly its service. After all users should register lots of accounts in different services and download lots of applications to have the opportunity for communication with all necessary people immediately.

The Internet which we know now exists due to open standards. All layers of network interaction, starting from the physical layer (transmission and reception of raw bit streams over a physical medium) to the application layer (HTTP, E-mail) are opened and accessible for anybody. Anybody can make his or her own web site, browser, e-mail client. But it is not protected.

That is why we have many operation systems, which can work with the Internet, and we have the variety of devices and applications that support popular protocols.

The question of building information technology for transmission encrypted data in modern mobile systems was investigated by foreign and domestic scientists: B. Holdshtein, A. Pinchuk, A. Sukhovyt'skyi, P. Sermos, A. Takanen, V. Polinovskyi, M. Houh.

There is a problem of creating distributed client-server systems with cryptographic protection in the application layer, which can support loads of users and provide appropriate protection of information.

The modern stage of data transmission development system in real-time and its high heterogeneity require from network equipment clear interaction and the ability to guarantee the qualitative data transmission from one network segment to another. One of the most perspective area in the development of such systems nowadays is creation of server base on IP protocol, which allows to create the real-time data transmission systems with agreement of requirement of information confidentiality. There are loads of information technologies, which are made for this aim. However, many of them cannot provide the appropriate level of data transmission protection with high quality of communications.

Therefore, the research started from the analysis of existing technologies for REST-server creating. This server provide encrypted messages and files transmission. Also, there was provided the analysis of databases for storing main information of the system.

During the work were offered new ways of server module services creation. They are based on the platform with open code Node.js. This gives us such advantages:

- Asynchronous singlethreading model of requests execution;
- Non-blocking input/output;
- Modules system CommonJS;
- Engine JavaScript Google V8.

Also, there were provided servers utilities for encrypted data transmission, Web client services for encrypted data transmission and visualization; developed new REST-server model due to using of asynchronous server platform NodeJs and NoSQL database MongoDB.

Individual modules were created by authors. These modules execute functionality of REST-server on the platform with an open code NodeJs for transmission and saving encrypted data. Server software was written on JavaScript. HTTPS and WebSocket protocols are used in services for transmission the data. Services use symmetric algorithm block ciphers Advanced Encryption Standard (AES) for encrypting messages with 256 bits